Identity and Access Management System Requirements in Health care, especially in Oulu University Hospital

S. Virkkunen *

- Northern Ostrobothnia Hospital District, Oulu University Hospital, Oulu, Finland
  sanna.k.virkkunen@gmail.com

Abstract

In this paper some basic information of Identity and Access Management and health care systems are discussed. These include e.g. basic dilemmas of identity and access management projects, digital identities, their roles, rules and groups, and processes in identity management.

Keywords: IDM, IAM, Identity and access management, processes, Federation, Provisioning, Health care, Single-sign-on.

1 Introduction

Patient data is considered as confidential, sensitive information. The mere information of an individual being a patient is considered secret. [1].

Identity and access management has not been systematically organised in different platforms until recent years. Identity and access management projects have had a bad reputation due to high failure rate. Projects have exceeded their budgets, as well as their schedules. In worst cases the identity and access management software has never been ready for deployment. However a successful IAM project improves security and productivity in the whole organisation as the costs in managing users and their attributes and credentials lower.

In Oulu University Hospital there are almost 150 different information systems. All these have different user accounts, user roles and passwords although some federation occurs. The vast amount of computer systems is about the same in every health care organization, small health centers being the exceptions.

2 Identity management requirements in health care

Identity and access management has a big role in the security and confidentiality of health care systems. Access rights The Decree of the Ministry of Social Affairs and Health on patient records claims that each individual employed in health care and user of electronic patient record has to have access rights that are being defined according to the current role of the individual. According to the decree it’s said each user has to have only the access rights that are needed for the job. Access rights have to be maintained with access management system. All the users of the patient information systems need to be identified and recognized in a way that users are verified unambiguously. [2]. In other terms it’s a necessity to use digital certificates in Population Register Centre’s smart cards for health care when using patient information.

KanTa auditing requirements claim the management of user rights in a health care information system concerning electronic prescription data has to be done with external system, e.g. identity and access rights management system. All the user rights and changes done to user rights have to be logged. The log file needs to be archived for 12 years after the resignation of the employee. Also permitting access rights and managing accesses has to be based on role based access rights, according to the KanTa auditing requirements. [3]

2.1 Identity management challenges in health care

In a health care organization identity management is widely spread. There are many users, many different roles, partners, customers and vendors that need to be taken care of. Alone in Oulu University Hospital there are 6800 employees, of which there are full-timers, part-timers, fixed term employees, inside substitutes, students, apprentices, civil servants and researchers.

In identity management in health care there are also several different target systems and archives: portals, Local Area Networks, email, remote accesses, as well as operative systems and services for outside customers. There can also be many electronic identities for one individual. The same person can be normal employer during the day, a practicing student during the evening and also a private practitioner occasionally. Also the same individual can appear several times in different
user registers and databases. These different roles and also short employment periods make the health care environment challenging for identity management.

2.2 Basics of Identity Management

Identity management can be roughly divided in user rights management, access management and provisioning. Each user has organizational roles depending of the organization the user is part of. The user also has roles business roles depending of the tasks the user is performing daily. The user can also have dynamic roles, e.g. “superior” or “super user”. Lots of user rights management automation can be done based on these rules but usually also additional attributes are used. Digital identity involves all these rules, attributes and other user information.

2.2.1 User Rights Management

User rights management answers to questions like “Who am I?” “What rights do I have?” “What is the basis for my rights?” “Who has accepted my rights?” To gain fully functionality of user rights management requires properly maintained and gathered master data.

2.2.2 Access management

Access management is about authentication, identification and authorization. It answers questions like “How do we control who is using our systems?” “In what manners our systems are being used?” “How can we make sure the user is the individual he/she claims to be?” Functionality of access management can be implemented using technologies such as repositories, meta-directories, databases, LDAPs and other directory services.

2.2.3 Provisioning

Provisioning means forwarding user information and user rights to service systems. This leads to the basic dilemma of maintaining all this information in different systems up to date in all times.

Provisioning can be automated or manual process. However with manual handling of user data the possibility of gaining all the needed log data and reconciliation lowers. With manual system there usually is also huge amount of manual work to be done with lost and forgotten passwords. Typically provisioning is done distributed in health care. This way there always has been some one close by creating user accounts for new, sudden employees in emergency situations.

Identity management is organization wide process. It includes controlling, modifying, accepting, declining and implementing all identity and user data. It also handles with self-service functions, work queues and maintenance services. One of the most important parts of identity and access management system functionality is to get life-cycle management for all identities.

2.2.5 Federation

In some cases even in health care it is reasonable to trust the authentication mechanism of a third party. This is called federation. A great example of federation is commonly used Haka-system in Finnish universities. In Haka web of trust the home university maintains all the basic data or master data of the student and authenticates the user e.g. with password. The home university then assigns the user data to service provider who then decides depending of the master data, what kind of view the user sees in the service. Haka is build mainly on Shibboleth open source software.

However in health care federation can’t be used in to this extent due to restrictions of health care legislation. In
order to use federation for example with other organizations patient record, the home organization would have to trust the way the different user rights, roles and accounts have been given in the other organization. Typically this would require agreeing on governance policies the other organization has made. It also would require all parties to understand the governance policies of the other organization.

![Figure 3: Haka](image)

**2.2.4 Single-Sign-On**

Also single-sign-on is often mentioned in identity and access management. Enterprise single-sign-on system usually consists of central server, which stores each user’s logins and passwords for multiple systems. Depending on the implementation of single-sign-on system, there usually is either single-sign-on agent running on each computer, sniffing if there is a login window opened or script-based programs, which have login data programmed inside the script.

![Figure 4: Enterprise Signle-Sign-On](image)

Using single-sign-on the user doesn’t need to remember any account information, single-sign-on does this for the user. Using single sign on with Population Register Centre’s smart cards reduces the time needed to log in to different systems. Only actual thing to remember is then the PIN code for the smart card. In elaborate system environment the enterprise single sign on system fills in all the login data needed.

**2.2.5 Auditing**

Proper auditing makes it possible to view integrated life cycle of each identity. It makes it possible to see precise rights and restrictions the user has had on each information system on a given date.

Auditing also makes it possible to run different reports from the system. In health care such reports could be dangerous work combinations. Dangerous work combination in health care happens for example when the same person has rights to order, approve and use heavy medication. Dangerous combinations typically consist of super users and acceptors.

**2.3 Drivers in identity management projects in health care**

Finnish legislation requires all the user rights in health care has to be maintained role based either within the health care systems or with identity and access management system. Proper auditing of the health care information systems requires full reconciliation has to be possible. There also has to be solid revision history of the events in user rights information. Using IAM systems also makes identity management processes more efficient in all areas of the process: requesting the user rights, accepting, declining and implementing them. Using enterprise-wide single sign-on system decreases the amount of remembering different user logins and passwords. In other words identity management system project is one of the few projects in health care that actually reduces the amount of time nurses have to spend with the computers.

**2.4 Master data**

Identity and access management cannot function without comprehensive master data management. In hospital identity management master data consists of the basic data of the personnel, customers, students and vendors. It can be data collected from HR systems but is often scattered in different information systems.

Master data is typically constant information, such as name and address data, superior information, and information concerning the organization structure. It can be used for example ERP systems. Master data has to be integrated to the target systems with e.g. identity and access management system. Master data helps restricting the access of the employee only to those information that he / she needs.

In a health care organization internal master data can be found in HR systems, recruitment systems, radiology
information systems, other information systems and in some paper forms. External master data is even more widely spread, e.g. in pharmacy systems, material management systems, in schools and universities for medicine and health care students and in paper forms.

Master data system has to be integrated to other systems. The information coming from HR and other source information systems typically forms a CSV file that will be read into master data. Master data then stores the data. Master data system can provide this information to other systems as well, e.g. identity and access management system. The crucial step is to trust only the information coming from master data. The route of the information will be cascade modeled. If the data in the master data system is biased, the whole identity process will be biased.

2.5 Electronic Forms

Due to the strict legislation, auditing requirements and high publicity value of the health care information, there are many forms for employees and supervisors to fill in case of new employment. The requirements of the legislation are being implemented with elaborate manual processes. This requires lots of remembering and great amount of paper forms. Manual processes lack the possibility to do advanced reporting for authorities.

To implement fully functioning identity and access management system in health care requires converting old paper forms in electronic format. This itself is a long process that needs clear vision and knowledge of law concerning health care. Without the electronic forms identity and access management system has no baseline.

2.8 Conclusions

Fully functioning IAM system reduces risks of processing digital identities in health care. Costs of resetting passwords manually will decrease as well as the amount of memory based access information needed from the users. New employee's orientation to new job will be easier and shorter due to automated access rights processes. Also the security risks of dismissal will lower.

However identity and access management system consists of many different parts and sections. Implementing identity and access management system is never ending job. It’s no wonder identity and access rights projects usually fail. Multi-dimensional, large-scale projects are difficult to keep in balance within money, time and quality.

References